IC, IC-MOUNTED ELECTRONIC DEVICE, DEBUGGING METHOD AND IC DEBUGGER

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to an IC, an electronic device, a method for debugging the IC, a method for debugging the electronic device, and a debugger, having a security function for preventing a spurious acquisition of a behavior of an internal circuit of the IC.

2. Description of the Related Arts

In every field such as an electronic commerce, etc., a device of higher security is demanded. For this reason, various methods for preventing a reverse engineering in the device are devised. However, irrespective of these trials, a reverse engineering ROM, or the like is prepared, and an abuse for a reluctant use for a developer of the device does not become extinct. For this reason, a system in which a third person is incapable of engineering operation itself of the device is demanded.

Fig. 9 is an explanatory diagram of the prior art. As shown in Fig. 9, an LSI 110 is provided with a CPU 200, a peripheral circuit 300, and a bus 600 for connecting therewith. In this LSI 110, the CPU 200 acquires data or programs from the peripheral circuit 300, and processes the data, and outputs them to the

peripheral circuit 300.

On the other hand, in the case where the device is developed by use of this LSI 110, a processing behavior of the CPU 200 is directly monitored, and the programs or the like are verified. A verification method for monitoring output data of the peripheral circuit 300 is executed, but a behavior of the CPU 200 up to the output cannot be elucidated from the output data.

For this reason, the CPU 200 is provided with a debug I/F (interface) circuit 400 via another bus 500. An external debug controller 100 of the LSI 110 is connected to the debug I/F 400, and supplies a clock CLK, and inputs a signal SIN, and obtains an output SOUT.

This debug I/F circuit 400 is exploited for acquiring a behavior (contents of a program counter, a register, or the like) of the CPU 200 at the time of developing the device, and in the case where the device is shipped to a field, the debug I/F circuit 400 is similarly exploited at the time of the occurrence of a fault, and at the time of diagnosing the device.

A security function is not provided in the prior art with respect to an access from the debug I/F 400, as described above.

In the device which does not require a conventional normal security, a debug I/F terminal is seen from outside irrespective of the time of being unused/the time of being used, and is entirely defenseless for the exploitation by the third person. For this reason, in the case of the device shipped to the field,

the third person uses the debug I/F terminal, so that a behavior of a central processing unit (CPU) can accurately and readily be made reverse engineering, and it needs high-performance in security.

However, in the case where the conventional device uses the CPU provided with the debug I/F function, a clue of analysis is given to the third person. For example, in the case of a POS register using the CPU with the debug I/F function, a debug unit of the debug I/F is connected to a personal computer, etc., so that even data such as a password, a cryptographic key, or the like can readily be searched.

SUMMARY OF THE INVENTION

It is therefore the object of the present invention to provide an IC, an electronic device, a debug method, and a debugger for restricting a use of a debug I/F and preventing a spurious reverse engineering by a third person.

It is another object of the present invention to provide an IC, an electronic device, a debug method, and a debugger in which an authentication logic is provided between the debug I/F circuit in the LSI and an external terminal, and a restriction is formed in exploiting the debug I/F.

It is yet another object of the present invention to provide an IC, an electronic device, a debug method, and a debugger for preventing the engineering of the authentication logic between the debug I/F circuit in the LSIs and the external terminal.

It is a further object of the present invention to provide an IC, an electronic device, a debug method, and a debugger for detecting the spurious reverse engineering by a third person which restricts the use of the debug I/F.

In order to attain the above objects, according to a first aspect of the present invention there is provided an IC comprising an internal circuit; a debug I/F circuit for debugging the internal circuit from externally; and an authentication circuit which is provided between the debug I/F circuit and a debug terminal, and when the debug I/F circuit is activated, transmits a transmission key from the debug terminal to outside, and authenticates from a signal received from the debug terminal and a transmission key, and enables operation of the debug I/F circuit.

According to a second aspect of the present invention there is provided an electronic device mounting with an IC, the IC comprising an internal circuit; a debug I/F circuit for debugging the internal circuit from externally; and an authentication circuit which is provided between the debug I/F circuit and the debug terminal, and when the debug I/F circuit is activated, transmits the transmission key from the debug terminal to outside, and collates the signal received from the debug terminal with the transmission key, and enables operation of the debug I/F circuit.

According to a third aspect of the present invention there is provided a debugging method comprising the steps of transmitting the transmission key to externally when the debug

I/F circuit is activated; and authenticating the signal received from externally and the transmission key to enable operation of the debug I/F circuit.

According to a fourth aspect of the present invention there is provided a debugger for debugging an IC, the IC comprising an internal circuit; a debug I/F circuit for externally debugging the internal circuit; and an authentication circuit which is provided between the debug I/F circuit and the debug terminal, and when the debug I/F circuit is activated, transmits the transmission key from the debug terminal to outside, and collates the signal received from the debug terminal with the transmission key, and enables operation of the debug I/F circuit, further comprising: the discrimination device which is provided between a debug unit and the debug I/F circuit, and receives the transmission key to encode it by a predetermined key, and transmits the reception signal.

Since an authentication circuit is provided between the debug I/F circuit and the debug terminal, it is possible to protect an internal circuit from a dishonesty as performing reverse engineering a motion of the internal circuit, etc. by exploiting the debug I/F of the third person, and to hold security higher than a conventional device.

Furthermore, since the security is performed by a physical connection and an authentication algorithm by a set of a discrimination device and an IC, the high security is enabled. Furthermore, a spurious engineering by a PC (personal

computer) is difficult.

Furthermore, in the debugging method according to the present invention, the authentication step has a step of canceling a reset signal to the debug I/F circuit for enabling of the operation. In the LSI according to the present invention, the authentication circuit cancels the reset signal to the debug I/F circuit for enabling of the operation. For this reason, even if authenticated, it is possible to realize by cancellation of the existent reset.

Furthermore, in the LSI according to the present invention, the authentication circuit forms an authentication key that is encoded the transmission key by a predetermined key, and compares the reception signal with the authentication key. In the debugging method according to the present invention, the authentication step has a step of forming the authentication key that is encoded the transmission key by the predetermined key, and of collating the reception signal with the authentication key. As encoded, the higher security is possible.

In the LSI according to the present invention, the authentication circuit awaits a time of the operation enabling. In the debugging method according to the present invention, the authentication step has a step of waiting a time of the operation enabling. Before and after judgment of a serial data key, a waiting time is provided after the end of agreement judgment by use of a timer. For this reason, even if the third person inputs any cryptographic key data, it takes much time

to obtain authentication results (reset). This causes to prevent the use of the spurious debug I/F by the third person, and furthermore when retrying several times, it takes enormous time.

In the LSI according to the present invention, the authentication circuit forms the transmission key with random numbers, whereby each time serial data (transmission key) to be transmitted are activated, the random numbers are based, so that the serial data are set as transmission and reception data different every time, rendering the analysis thereof difficult.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of an LSI according to an embodiment of the present invention;

Fig. 2 is an explanatory diagram of an authentication processing of Fig. 1;

Fig. 3 is an explanatory diagram of a debugging method of the LSI of Fig. 1;

Fig. 4 is an explanatory diagram of preventing a spurious access to the LSI of Fig. 1;

Fig. 5 is an explanatory processing of another authentication processing of Fig. 1;

Fig. 6 is an explanatory diagram of an electronic device mounting the LSI of Fig. 1;

Fig. 7 is a block diagram of a peripheral circuit of Fig. 1;

Fig. 8 is a configuration diagram of a POS system mounting the LSI of Fig. 6; and

Fig. 9 is an explanatory diagram of the prior art.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The preferred embodiments of the present invention will now be described by sorting it into a LSI, an electronic device, and other embodiments.

[LSI]

Fig. 1 is a block diagram of an LSI and a debug mechanism according to a first embodiment of the present invention, and Fig. 2 is an explanatory diagram of the authentication processing, and Fig. 3 is a diagram for explaining operation at the time of a due use, and Fig. 4 is a diagram for explaining operation at the time of a spurious use.

In Fig. 1, reference numeral 2 denotes a system LSI with a CPU, and a debug I/F utilization authentication circuit according to the present invention is provided to the LSI 2. Reference numeral 1 denotes an external debug controller for utilizing the debug I/F inside the LSI 2. Reference numeral 3 denotes a discrimination device, which is used by interposing it between the LSI 2 and the debug controller 1, so as to interlock with the authentication circuit inside the LSI 2 and authenticate.

The LSI 2 has a debug I/F circuit 2-1, a CPU 2-2, a debug bus 4-1 for connecting an I/F circuit 2-1 and the CPU 2-2, and a peripheral circuit 2-12 connected to a CPU bus 4-2. The

peripheral circuit 2-12 is different according to the use of LSIs, for example, an electronic money funds transferring circuit that will be explained in Fig. 6 on.

In the embodiment of the present invention, the authentication circuit is provided in this CPU bus 4-2. A structure of the authentication circuit is explained.

A port 4-2 receives write data of the CPU 2-2 from the bus 4-2. A register 2-5 stores a debug I/F utilization transmission key formed by the CPU 2-2. A register 2-8 stores an authentication key formed by the CPU 2-2. A transmission circuit 2-4 transmits the transmission key of the register 2-5 in synchronism with a clock supplied by the discrimination device 3. A shift register 2-6 receives a cryptographic key returned from the discrimination device 2.

An agreement detection circuit 2-9 compares a cryptographic key of the shift register 2-6 with an authentication key of a register 2-8, and detects an agreement. A timer circuit 2-7 starts counting clocks in response to an agreement detection output of the agreement detection circuit 2-9, and forms a signal for canceling a reset signal to the internal debug I/F circuit 2-1 after a constant time. A reset gate 2-11 cancels an input to the debug I/F circuit 2-1 of the reset signal according to a reset cancellation signal. A reception-enabling gate 2-10 enables the shift register 2-6 which fetches in data from a signal input terminal SIN in response to a reception-enabling signal from a transmission circuit 2-4.

Next, the discrimination device 3 is provided with a key reception circuit 3-1. When the discrimination 3 is turned on, the key reception circuit 3-1 transmits clocks and receives the aforesaid transmission key, and encodes it by a key determined previously and transmits the cryptographic key.

Next, an operational procedure capable of utilizing the debug I/F will be explained with reference to Figs. 1 and 2. As shown in Fig. 1, the debug controller 1 utilizing the debug I/F is connected to the LSI 2 via the discrimination device 3.

① First, the LSI 2 and discrimination device 3 are turned on and activated. Then, a clock is supplied from the discrimination device 3 to the debug I/F 2-1 of the LSI 2. Concurrently, the CPU 2-2 is activated in the LSI 2, and the LSI 2 forms the debug I/F utilizing transmission key and authentication key by a firmware, and writes them into the registers 2-5, 2-8 via the bus 4-2 and port 2-3. At this time, the transmission key is formed based on a random number, and then the authentication key is generated by encoding the transmission key by a predetermined key.

② When the key is written, the transmission circuit 2-4 transmits the transmission key in synchronism with a clock supplied by the discrimination device 3.

③ The key transmission and reception circuit 3-1 in the discrimination device 3 receives the transmission key, and encodes the transmission key by the key determined previously, and transmits the cryptographic (encoded) key. The

predetermined key at this time is same as the key used a little while ago by the firmware in the LSI 2.

④ In the LSI 2, the shift register 2-6 receives the returned the cryptographic key, and the agreement detection circuit 2-9 compares it with the authentication key of the register 2-8, and only in the case where agreed, the agreement detection circuit 2-9 transmits the agreement detection to the timer circuit 2-7. The timer circuit 2-7 waits for a constant time, and canceled a reset signal to the internal debug I/F 2-1 by the gate 2-11.

Thus, for the first time, the debug I/F circuit 2-1 of the LSI 2 can be utilized. Namely, the reset signal is transmitted from the debug controller 1 to the LSI 2, and resets the debug I/F circuit 2-1, and utilizes the debug I/F circuit 2-1, and can access the CPU 2-2.

As shown in Fig. 3, a LSI provider offers the LSI 2 and discrimination device 3 to a developer for an apparatus. The encryption key of the LSI 2 is same with the encryption key of the discrimination device 3. The developer mounts the LSI 2 on the target board 7, and develops the device.

In the case where the debug is performed, the LSI 2 is connected to the discrimination device 3, which is connected to the debug controller 1, the PC interface board 6, and the personal computer 5. When the discrimination device 3 intervenes therebetween, the above authentication sequence works to cancel a reset, so that the debugger on the PC 5 can utilize the debug I/F circuit 2-1. Furthermore, even after

the device is shipped to a field, the discrimination device 3 is connected, thereby utilizing the debugger on the PC 5.

On the other hand, as shown in Fig. 4, in the case where the discrimination device 3 is not connected, the reset is not canceled in the debug I/F circuit 2-1 of the LSI 2, and the debugger of the PC 5 cannot access the CPU 2-2 of the LSI 2. For example, after the device is shipped to the field, it is possible to protect the CPU 2-2 from dishonesty such as reverse engineering of internal operation of the CPU 2-2 by utilizing the debug I/F of the third person, and to hold the higher security than the conventional device.

Namely, in a security technique such as a conventional password authentication, etc., if the password is leaked, the security function is not performed, and the password is easy to elucidate by retrying. Accordingly, the security technique is unfit as a security mechanism of the LSI 2 to be presented to a great number of users. According to this embodiment, since in order to realize the security with a set of the discrimination device 3 and LSI 2, the security is carried out by the physical connection and authentication algorithm, the high security is enabled. Furthermore, the spurious engineering by the PC 5 is difficult.

Furthermore, in some cases, since the aforesaid utilization authentication function is an encryption algorithm, a skillful spurious person knows existence of the authentication mechanism and tries the engineering by retrying the encryption key (data). According to this embodiment, since

this engineering becomes difficult, the next technique is adopted.

First, after the serial data key is judged, waiting time is provided after end of the agreement judgment by use of the timer 2-7. For this reason, even if the third person inputs any cryptographic key data by connection of Fig. 4, it takes much time until obtaining authentication results (reset). Thus, the spurious debug I/F utilization by the third person is prevented, and it takes enormous time when retrying several times.

Second, each time the serial data (transmission key) to be transmitted are activated, the random numbers are based, so that the engineering becomes difficult as set as transmission and reception data different each time.

Third, the reception operation of the shift register is conducted for a constant time after the transmission key is transmitted, and only one time reception is made at the time of one time activation, and since if data are repeatedly input, not accepted, the engineering is difficult.

Next, in Fig. 5, the authentication processing according to another embodiment of the present invention will be explained.

① First of all, when the LSI 2 and discrimination device 3 are turned on, a clock is supplied from the discrimination device 3 to the debug I/F 2-1 of the LSI 2. Concurrently, in the LSI 2, the CPU 2-2 is activated to form the debug I/F utilization transmission key and authentication key by the

firmware, as described above, to write them into the registers 2-5, 2-8 via the bus 4-2 and the port 2-3.

② When the key is written, in synchronism with the clock supplied by the discrimination device 3, the transmission circuit 2-4 transmits the transmission key.

③ The key transmission and reception circuit 3 in the discrimination device 3 receives the transmission key, and encodes the transmission key by the key determined previously, and transmits the cryptographic (encoded) key. The predetermined key at this time is same with the key used a little while ago by the firmware in the LSI 2. The discrimination 3 annexes a user ID and transmits it to the LSI 2.

④ In the LSI 2, the shift register 2-6 receives the returned cryptographic key, and the agreement detection circuit 2-9 compares it with the authentication key of the register 2-8, and only in the case where agreed, the agreement detection circuit 2-9 transmits the agreement detection to the timer circuit 2-7. After the timer circuit 2-7 waits for a constant time, the timer circuit 2-7 cancels an input of the reset signal to the internal debug I/F 2-1 of the gate 2-11. Furthermore, the user ID is logged. For this reason, if information of the transmission key should be leaked, it is possible to specify which user has leaked, from the logged user IDs.

According to the embodiment of the present invention, the description device 3 adopts a method of encoding the received transmission key and use ID by the key, thereby preventing

that the user ID is readily changed.

[Electronic Devices]

Next, electronic devices mounting the aforesaid system LSI 2 will be explained. Fig. 6 is an explanatory diagram of an example to which the system LSI 2 is applied, and Fig. 7 is a structural diagram of a peripheral circuit of the LSI 2 in this application example, and Fig. 8 is an explanatory diagram of the electronic devices.

As shown in Fig. 6, the system LSI 2 is a card funds transferring LSI, and has a debit card funds transfer function 40, a credit card funds transfer function 41, an electronic money funds transfer function 42, and other service functions 43. For this reason, the LSI 2 is connected to an IC card reader/writer 30, a magnetic card reader 31, and a display and key 32. Furthermore, as occasion arises, the LSI 2 is connected to a receipt printer 33. These funds transfer functions 40 to 43 are realized by execution of the programs of the CPU 2-2 of the LSI 2.

Accordingly, by mounting this LSI 2, a card funds transfer function is imparted to various electronic devices 50 to 57. These electronic devices are, for example, a POS (point of sales) reader/writer 50, an integrated terminal 51, a mobile terminal 52, an ATM (automatic teller machine) 53, an automatic vending machine 54, a PDA (personal digital assistant) 55, a portable telephone 56, and a PC (personal computer) 57.

The peripheral circuit 2-12 of the LSI 2 for the card funds transfer will be explained with reference to Fig. 7.

The peripheral circuit 2-12 has a smart card controller 60, a MS (Magnetic stripe) control circuit 61, a LCD control circuit 62, a matrix KB control circuit 63, a memory controller 64, and serial I/O ports 69 to 72. In Fig. 7, the above LSI 2 indicates a condition of being mounted on the target board 7, and for clarity of description of the LSI 2, only the CPU 2-2 and peripheral circuit 2-12 (60-64, 69-72) are shown. Of course, the LSI 2 includes the debug I/F 2-1 and the authentication circuit.

The smart card controller 60 reads/writes data of the IC card (called a smart card) via the IC card reader/writer 30. The MS control circuit controls the MS (magnetic stripe) reader 31. The LCD control circuit 62 controls a display of the LCD (liquid crystal display) 32-1. The matrix KB control circuit 63 recognizes an input of a ten key 32-2. The memory controller 64 control an input/output into/from various memories (a ROM 65, a SRAM 66, a FLASH 67, a SDRAM 68) on the board 7. The serial ports 69 to 72 are connected to drivers 73 to 75 of the port 7 for inputting and outputting the serial data. These are each connected to the CPU bus 4-2.

Fig. 8 is a system configuration diagram of the electronic device mounting a funds transferring LSI, showing a POS (point of sales) system. The network 35 is connected to a store controller 20 and a plurality of POS terminals 10. The POS terminals 10 are connected to the IC card reader/writer 30. The store controller 20 and the plurality of POS terminals 10 are provided with the above funds transferring LSIs (called

an IFD), which exchanges directly funds transfer data.

An IC card 34-1 for customers is exchanged messages with a POS IC card 34-2 via the IFD 2, and the POS IC card 34-2 is exchanged messages with the IC card 34-2 of the store controller 20 via an IFD 2, a terminal controller 11, a network 35, the terminal controller 11, and the IFD 2.

For example, in the case where the electronic funds transfer is carried out by the IC card, a customer's data of the IC card 34-1 are stored in the POS IC card 34-2 via the IFD 2. Thereafter, the stored data of the POS IC card 34-2 are stored in the IC card 34-2 of the store controller 20 via the IFD 2, the terminal controller 11, the network 35, the terminal controller 11, and the IFD 2.

In this system, as a route of the electronic funds transfer data is closed by the IFD 2, there is no fear that funds transfer data (a password, an accounting number, a balance, and the like) are leaked. Therefore, safety is high.

However, as described above, if accessing the CPU 2-2 by utilizing the debug I/F, it is possible to make a spurious acquisition of funds transfer data (a password, an accounting number, a balance, and the like), so that there is a fear of abusing. Accordingly, an authentication mechanism according to the present invention is, in particular, valid for such uses.

[Other Embodiments]

In addition to the aforesaid embodiments, the following modifications according to the present invention are possible:

(1) According to the aforesaid embodiments, the reset signal is canceled by the authentication, but a gate may be provided at a clock input side of the debug I/F 2-1, so that a clock input is enabled by the authentication.

(2) According to the aforesaid embodiments, the waiting time are provided by the timer after the agreement judgment, but the waiting time may be performed for the judgment by the timer before the agreement judgment.

(3) In the case where the disagreement is detected by the agreement judgment, this can be notified to the peripheral circuit. Thus, the peripheral circuit judges as a spurious access, and for example, it is possible to make a disposition such as erasing of data required for the security.

(4) The system LSI is explained for the card funds transfer, but it may be used as the other applications.

(5) The explanation is made as the debug I/F of the CPU, but the present invention can be applied to the debug I/F of the other circuits.

Although the present invention has been described in light of the preferred embodiments thereof, the present invention could be variously modified without departing from the sprit of the present invention, and those modifications are not to be excluded from the scope of the invention.

As set forth hereinabove, according to the present invention, the following effects are presented.

Since the authentication circuit is provided between the debug I/F circuit and the debug terminal, it is possible

to protect the internal circuit from dishonesty such as the reverse engineering, etc. of operation of the internal circuit by utilizing the debug I/F of the third person, and to hold the security higher than the conventional device.

Furthermore, since the security is carried out by the physical connection and authentication algorithm with a set of the discrimination device 3 and LSI 2, therefore, the high security is enabled. Furthermore, the spurious engineering by the PC 5 is difficult.